TESTIMONY OF JOHN STREUFERT,
ACTING CHIEF INFORMATION OFFICER,
U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID)

BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM ON THE STATUS OF FEDERAL AGENCIES' IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

April 7, 2005

Chairman Davis and Members of the Committee, I want to thank you for the opportunity to testify on the status of USAID's Information Systems Security Program and our implementation of the Federal Information Security Management Act (FISMA). We appreciate your interest, and look forward to close cooperation with you and your committee as USAID continues to improve our Information Systems Security Program.

I would like to begin by describing USAID's mission and the unique information system security challenges created by this mission. Then I would like to report to you on how our risk-based Information Systems Security Program has successfully implemented FISMA. Lastly, I will provide a recent example of how this risk-based approach allowed USAID the flexibility to respond to the December 2004 tsunami.

USAID's Unique Mission Drives Our Information Systems Security Program

USAID was created as an independent agency in 1961 by the Foreign Assistance Act. Since that time, USAID has been the principal U.S. agency to extend assistance to countries recovering from disaster, trying to escape poverty, or engaging in democratic reforms. USAID fosters long-term and equitable economic growth and advances U.S. foreign policy objectives by supporting: economic growth, agriculture, and trade; global health; and democracy, conflict prevention, and humanitarian assistance.

Our headquarters is here in Washington, D.C., with field offices in more than 70 countries around the world. To achieve our mission, USAID works in close partnership with many different Private Voluntary Organizations (PVOs), indigenous organizations, universities, American businesses, international agencies, other governments, and Non-Governmental Organizations (NGOs).

USAID's mission requires us to work in developing countries; this creates many challenges for implementing a worldwide Information Systems Security Program. The information technology and telecommunications infrastructure in most of the countries where USAID does its work are not as robust or dependable as the infrastructure here in the United States. Yet, work with our development partners compels us to work with and be part of this developing infrastructure. Some of the information technology infrastructure challenges in these developing countries include: unreliable power grids, non-existent fiber optic connections, expensive bandwidth, and high latency. Furthermore, we rely on locally trained staff to manage USAID's systems at each of our field offices as well as to provide help desk support to the 6,000 workstation users in our field offices around the world.

This means that the risk environment in which USAID operates is unique.

Although USAID operates three separate computer networks (each supported by a different risk model), most of the USAID information technology activity occurs on AIDNET, which is a single worldwide network made up of 8,000 interconnected workstations and 7,000 other network infrastructure devices. Approximately 2,000 of the workstations are here in Washington with the remaining 6,000 workstations located in more than 70 countries around the world.

AIDNET is a very active network. We receive approximately 2 million emails a month and block the 500,000 of those emails that are spam. We also block more than 150,000 viruses each month. USAID's firewalls are located at more than 50 sites around the world but are managed and controlled in Washington, D.C. The firewalls handle more than 11 million access attempts each day and deny 4 million of those attempts. We have approximately 36,000 web pages on our public web site and 20,000 web pages on our intranet. The public pages are accessed more than 6 million times a month and the internal pages are accessed more than one million times a month.

Risk-Based Program to Protect the Confidentiality, Integrity, and Availability of USAID Information Resources

Our Information Systems Security Program uses a risk-based management model that requires us to support our business decisions with information security metrics. To support this model, we focus on computer security awareness. We deploy security data collection technology to provide risk measurements. We report this information to agency business system owners and decision makers in near real-time. These technologies provide us in-depth visibility into the daily operations of our global network and increase security awareness among USAID managers and staff. This risk-based approach is the only model with which we feel USAID can meet the challenges of today's dynamic security landscape. I would now like to discuss some of these technologies specifically and describe how each supports our risk-based approach to managing information security.

USAID uses an automated, daily security awareness tool called Tips of the Day to deliver training to employees and contractors worldwide. Every day during user login, the tool provides a brief lesson on computer security and then poses a security question that the user must answer to complete the login process. The tips are generated randomly for each individual, so typically our users do not receive the same tips. Last year we completed the worldwide deployment of the Tips of the Day program, and we were able to produce accurate metrics on the actual number of employees receiving this training. During fiscal year 2005 we will begin grading the user responses and reporting those grades to agency managers. These daily tips achieve precisely the results desired from awareness training – they reinforce the importance of computer security at USAID. Every user, including senior management, receives this daily computer security awareness training. Information security awareness, at all levels of USAID, is the foundation on which our Information Systems Security Program is built, and we plan to continue enhancing and improving our computer security awareness program.

If awareness training is the foundation, an important pillar of our Information Systems Security Program is vulnerability management. By understanding our vulnerabilities, we can measure the amount of risk we accept on a day-to-day basis. Our vulnerability management software continually scans our network (24 hours a day, 7 days a week). The 15,000 devices on our network are scanned, on average, 10 times a month. This scanning provides a continually updated status of our vulnerability posture to system managers and Information Systems Security Officers. In addition, we have developed a monthly grading system to help senior managers better understand their risk posture. We report these grades each month, on an A to F scale, to more than 90 system and application owners (these owners are senior managers in USAID). We also send executive summaries to the bureau heads and other senior managers in USAID. For example, we provide an Africa regional report to the Assistant Administrator for the Africa Bureau. This report summarizes all mission information systems security vulnerabilities and allows the bureau to determine needs for resource allocations. We also provide the Chief Financial Officer with monthly reports grading the security of all the systems around the world that are running major financial applications. Our capability to accurately measure and report in a timely manner the vulnerability status of our systems has been an effective method of managing our information systems security. Over the last twelve months we have significantly reduced the enterprise vulnerability posture; this is reflected in the grades provided to managers. The overall vulnerability assessment grade for the agency as an enterprise has moved from a C to an A.

Even though we have reduced our network-based vulnerabilities, we understand that security is a moving target. We cannot mitigate all the risks any more than we can stamp out all the possible vulnerabilities. Network threats exist. To combat this reality, we have deployed a global network of security devices that transmit security event information to a central collection, correlation, and reporting system called a Security Information Management system (SIM). This SIM collects suspicious security events and anomalies from hundreds of security devices and firewalls deployed throughout the enterprise. By collecting all our security events in the SIM database, we are able to correlate events across all disparate security device types within the enterprise, a powerful and critical tool when managing incident response on a global network. With daily reviews and active monitoring, we can identify and quickly respond to new information technology security threats and virus attacks. The technology also supports our incident reporting to US-CERT at the Department of Homeland Security, which provides important information to the rest of the federal community.

USAID has completed the certification and accreditation of all our major applications and systems. The certification and accreditation process used by USAID provides a regular and recurring review of all our major applications and systems. The certification of major applications and systems is done through my office by the USAID

Information System Security Officer (ISSO) which ensures that all major information technology investments receive a consistent view of risk information.

Part of the role of the Information Systems Security Officer is to make sure that the business system owners understand all the identified risks and the resource requirements associated with implementing the planned mitigation strategies. System accreditation is the responsibility of the business system owner. Who better understands the business requirements, what risks may be acceptable, or whether it is more cost-effective to mitigate a risk with a manual control than the business owner supporting the investment? In our experience, business owners, when they understand the risks, apply their resources to effectively mitigate and manage the identified risks.

The accreditation process requires the business owner to determine if the residual risk to agency operations, agency assets, or individuals is acceptable. If the risk is acceptable, an authorization to operate the system is issued and a plan of action and milestones for mitigating any residual risks is established. The Plan of Action and Milestones for each investment informs the USAID's Capital Planning and Investment Control (CPIC) committee of the current risk posture of the agency's steady state investments. This process provides a mechanism for the CPIC to consider security and risk factors before making investment funding decisions. USAID's Business Transformation Executive Committee serves as the Agency's CPIC authority.

How the USAID Risk-Based Approach Allowed USAID to Respond to the Recent Tsunami

Allow me to provide a recent important example of our risk-based approach to information security and how this approach supported USAID decision-making to quickly respond to the needs of those affected by the tsunami. As you know, USAID has the responsibility for managing the U.S. Government's response to natural disasters that occur around the world. Internally, this effort is managed by USAID's Office of Foreign Disaster Assistance (OFDA). OFDA's work environment is very different than that of the programmatic bureaus in the Agency that typically work on long-term development projects in our field offices overseas. OFDA must respond quickly to disasters that occur anywhere in the world. It must be mobile and agile to respond to emergencies in remote areas. OFDA's response teams operate at the site of the emergency and do not always operate from USAID's field offices.

As a result, the OFDA network uses a risk model different than AIDNET. The OFDA risk model stresses the importance of system availability over system confidentiality. This model allows OFDA to pre-position and pre-deploy systems to ensure rapid response to disasters and emergencies anywhere in the world.

Because of the different OFDA risk model and operational requirements, USAID created a network called OFDANET that is separate from AIDNET. In FISMA parlance, OFDANET is a separate General Support System (GSS) with its own Certification and Accreditation.

In December 2004, OFDA was called upon to provide relief in countries that were devastated by the tsunami. In responding to this disaster, OFDA quickly deployed Disaster Assistance Response Teams (DARTs) to the affected areas using computers and laptops that had been pre-positioned in Asia. With the OFDA computers in place, these teams were able to begin assessments and move funds to provide food and medical supplies to the needed areas immediately.

However, the enormous scale of this disaster also required that our USAID missions in this region rapidly add staff and computers to support the long-term rebuilding efforts. For example, the USAID mission in Sri Lanka, one of the hardest hit areas, added dozens of new computers to AIDNET. Our system administration staff, led by systems manager Anil Liyange, worked around the clock to provide the information systems infrastructure to support the United States government relief efforts in the region. Our other missions in the affected areas also needed to expand the number of workstations on their networks as well.

Any time there is an unplanned increase in the number of systems connected to the network, additional risk is introduced. Because USAID continually measures the system risks to its enterprise, we were able to make an informed and rational decision to allow this rapid, unplanned expansion of AIDNET and accept the added risk in order to meet our emergency business requirements. Further, we could report and track this risk until mitigated to an acceptable level.

In this instance, a compliance-based approach to information security may have hindered our ability to respond to the tsunami. Despite the differences between the AIDNET and OFDANET risk models, USAID's Information Systems Security Program promotes secure business decisions. This risk-based approach enables us to meet our FISMA responsibilities and enhances our ability to accomplish USAID's mission.

In summary, USAID's mission presents unique information security challenges. We have responded to these challenges by establishing a risk-based Information Systems Security Program that emphasizes computer security awareness, and deploys technologies to continually measure and report risk to the business and program executives. We will continue to adapt and improve our program as new regulatory guidance is published and as new security and information system technologies are developed. Our Information Systems Security Program enables USAID to work in a unique environment while protecting the confidentiality, integrity, and availability of USAID information resources.

I appreciate the opportunity to appear before you today and I would be pleased to answer any questions that you may have.